

Rec'd PCT/PTO 14 APR 2005

PCT/IB 03/04174

19.09.03

REC'D 03 OCT 2003

WIPO

PCT

PA 1047554

# THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

August 04, 2003

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: 60/467,040

FILING DATE: May 01, 2003

## PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

By Authority of the  
COMMISSIONER OF PATENTS AND TRADEMARKS



*P. Swain*

P. SWAIN

Certifying Officer

BEST AVAILABLE COPY

Please type a plus sign (+) inside this box

+

PTO/SB/16 (02-01)

Approved for use through 10/31/2002. OMB 0851-0032

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

Express Mail Label No. EV335816472US

Date of Deposit: MAY 1, 2003

## INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
QIONG S. MIHAELA	LI VAN DER SCHAAR	CORTLANDT MANOR, NY OSSINING, NY

☒ Additional inventors are being named on the page 2 separately numbered sheets attached hereto

## TITLE OF THE INVENTION (280 characters max)

SYSTEM AND METHOD FOR PROVIDING ERROR RECOVERY FOR STREAMING FGS ENCODED VIDEO OVER AN IP NETWORK

## CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ Customer Number

24737

OR

Type Customer Number here

**\*24737\***

☐

Firm or  
Individual Name

Address

Address

City

State

ZIP

Country

Telephone

Fax

## ENCLOSED APPLICATION PARTS (check all that apply)

☒ Specification Number of Pages

18

☐ CD(s), Number

☒ Drawing(s) Number of Sheets

2

☐ Other (specify)

☐ Application Data Sheet. See 37 CFR 1.76

## METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fees

FILING FEE  
AMOUNT (\$)

☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:

14-1270

160.00

☐ Payment by credit card. Form PTO-2038 is attached.

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: \_\_\_\_\_

Respectfully submitted,  
SIGNATURE

Date 1 May 2003

TYPED or PRINTED NAME

DICRAN HALAJIAN

REGISTRATION NO.: 39,703  
(if appropriate)

Docket Number:

US 020394

TELEPHONE

(914) 333-9607

## USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C., 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

03467040 05011

# **PROVISIONAL APPLICATION COVER SHEET**

**Additional Page**

PTO/SB/16 (02-01)

Approved for use through 10/31/2002. OMB 0651-0032

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Docket Number		US020394 US020394	Type a plus sign (+) inside this box →	+
INVENTOR(S)/APPLICANT(S)				
Given Name (first and middle (if any))	Family or Surname	Residence (City and either State or Foreign Country)		
RICHARD	CHEN	CROTON-ON-HUDSON		

Number 2 of 2

**WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

## **SYSTEM AND METHOD FOR PROVIDING ERROR RECOVERY FOR STREAMING FGS ENCODED VIDEO OVER AN IP NETWORK**

The present claimed invention relates to the field of streaming media data,  
5 particularly scalably encoded data. More specifically, the present claimed invention  
relates to the protection of such data.

Video transmission or video streaming within communication networks, such as  
ISDN networks or the Internet has become an important application of such  
communications networks. In the future, packet oriented mobile networks like GPRS  
10 (General Packet Radio Service) and UMTS (Universal Mobile Telecommunications  
Standard/System) will be commonly used to connect mobile users to fixed  
communication networks like the above-mentioned ISDN networks or the Internet. It is  
therefore important to employ efficient and intelligent support of high quality video  
streaming into wireless radio networks.

15 The problem of error concealment in video communications is becoming  
increasingly important because of the growing interest in the delivery of compressed  
video over wireless channels. Several packet-oriented transmission modes have been  
proposed for next generation wireless standards like EGPRS (Enhanced General Packet  
Radio Service) or UMTS, which are mostly based on the same principle: Long message  
20 blocks, typically IP packets that enter the wireless part of the network, are split up into  
segments of desired length, which can be multiplexed onto link layer packets of fixed  
size. The packets are then transmitted sequentially over the wireless link, reassembled,  
and passed on to the next network element. However, compared to the rather benign  
channel characteristics of present day fixed or wire line networks, wireless links suffer  
25 from severe fading, noise, and interference conditions in general, thus resulting in a  
relatively high residual bit error rate after detection and decoding.

Two types of error-recovery methods are commonly used to support video  
streaming over both wired and wireless networks: retransmission and forward-error  
correction (FEC). FEC coding is a well-known technique for achieving error correction  
30 and detection in data communications. FEC has the disadvantage of increasing  
transmission overhead and hence reducing usable bandwidth for the payload data. Thus it

is generally used judiciously in video services, since video services are very demanding in bandwidth but can tolerate a certain degree of loss. The retransmission method has the advantage of high bandwidth utilization, but suffers from long recovery delays which may not be tolerable for applications having strict delay constraints.

5        In the past, there has been a distinct line between utilizing one or the other method. An application design chooses either retransmission or FEC. However, IP based networks, are heterogeneous and evolving. It is conceivable that applications could operate in completely different network environments, making the network conditions hard to predict. This situation makes it difficult to choose the right error-recovery  
10    method for all possible operating scenarios.

An ideal solution for error-recovery would be to combine retransmission and FEC to thereby allow an application to dynamically choose one or the other, or rather combine them in real-time according to perceived network conditions.

Hybrid ARQ and adaptive FEC are two methods which combine the strengths of  
15    retransmission and FEC. In hybrid ARQ, the video data is pre-encoded by some FEC coding scheme, such as a Reed-Solomon coding scheme, and then the sender and receiver use a specially designed ARQ-like protocol to perform the protection. In adaptive FEC, FEC data is separated from original media streams, and "join"/"leave" commands are employed to achieve adaptive protection. However, adaptive FEC is limited in two ways.  
20    First, it uses Internet Group Management Protocol (IGMP) to signal the join/leave action, which may introduce a very long latency in the signaling process that eventually defeat the protection purpose, such as retransmission. Second, while it emphasizes the FEC coding algorithm, it lacks an architecture and protocols to carry out the goals of adaptive FEC.

25        It would be an advance in the art to provide a realistic architecture that specifies the protocols that are necessary for carrying out adaptive and efficient protection, thereby allowing applications to switch between different protection strategies dynamically.

In accordance with certain aspects of the present invention, methods and apparatuses are provided which allow a receiving device (client) to dynamically elect to  
30    receive protection data and determine the type of protection data to be received.

For example, in accordance with certain exemplary implementations of the

present invention, a method is provided for use in a server and a corresponding receiving device in communication with the server. The method includes the acts of: a first coding act for producing an encoded base layer from the bit stream using a frame prediction coding technique; a second coding act for producing an encoded enhancement layer from the bit stream using a fine granular scalable (FGS) coding technique; a first generating act for generating at least one protection bit stream; a second generating act for generating a first base layer hinting bit stream; a third generating act for generating a first enhancement layer hinting bit stream; and a fourth generating act for generating a first protection hinting bit stream.

10       According to another aspect, the present invention is a system that includes: means for producing an encoded base layer from the bit stream using a frame prediction coding technique; means for producing an encoded enhancement layer from the bit stream using a fine granular scalable (FGS) coding technique; means for generating at least one protection bit stream; means for generating a first base layer hinting bit stream; 15 means for generating a first enhancement layer hinting bit stream; and means for generating a first protection hinting bit stream.

The proposed error protection method and apparatus, referred to herein as on-demand protection, provides a number of advantages over the prior art, including: (1) The method may be advantageously fitted into an overall FGS streaming architecture; (2) The method supports both multicast and unicast applications; (3) The method takes full advantage of the MPEG-4 file format, thereby allowing a general-purpose MPEG-4 server to perform adaptive error protection to streaming applications; (4) Protection data is separated from protected data. In this manner, changing the protection data can change the protection level or strategy, but the protection procedures remain the same; (5) The method allows applications to dynamically choose between retransmission-like protection or FEC-like protection or hybrid ARQ, thereby gaining better protection performance; (6) The method uses Real-time Transport protocol (RTSP) instead of Internet Group Management protocol (IGMP) which can achieve faster protection and provide more flexibility to applications.

30       Referring now to the drawings where like reference numbers represent corresponding parts throughout:

FIG. 1 illustrates an exemplary network for performing end-to-end transmission of streaming media in which the present invention may be embodied; and

FIG. 2 illustrates, by way of example, an architecture and associated protocols for implementing the protection scheme of the invention.

5       The following terms are defined to better understand the present invention:

Streaming media - essentially mean real-time or near-real-time delivery of critical content (e.g., audio and/or video data) to a subscribing user's client device or devices. The client device/devices render the streamed media in a way that is appropriate for the client device and the media.

10       RTP protocol - It is used as the standard real time-based packetization-method in many environments and sits just above transport layers in a protocol stack, such as UDP (User Datagram Protocol)/IP(Internet Protocol). Generally, RTP is a transport protocol for real time data, and provides a timestamp, sequence number, data loss detection, security, content identification, and other data relevant to real time data delivery. RTP  
15       can be used in a unicast or multicast context.

RTSP protocol - an application-level protocol, which stands for Real Time Session Protocol, has been also developed to offer session negotiation and content description mechanism. RTSP describes how to stream the content from a server to a client. Streaming comprises breaking content into packets having sizes amenable (with  
20       respect to intermediate network characteristics) to transmission between the server and client.

FEC - Forward error correction is a well-known error correction technique which provides a mechanism by which a sending device provides a receiving device with additional FEC data that can be subsequently used by the receiving device to detect and  
25       correct errors in received data. Thus, to support FEC the sending device typically includes an FEC encoder and the receiving device typically includes an FEC decoder. FEC allows for different levels of encoding. The different levels of encoding can be expressed by a density ratio based on the amount of FEC data generated for a given amount of data. Thus, for example, in certain systems the FEC encoding level may be  
30       "high" when there is a ratio of one FEC packet for every data packet. In other systems,

the FEC encoding level may be "lower" such that there is a ratio of one FEC packet to every four data packets.

In the following description, for purposes of explanation rather than limitation, specific details are set forth such as the particular architecture, interfaces, techniques, etc., in order to provide a thorough understanding of the present invention. For purposes of simplicity and clarity, detailed descriptions of well-known devices, circuits, and methods are omitted so as not to obscure the description of the present invention with unnecessary detail.

It is assumed herein that the Real-time Transport Protocol (RTP) and the Real Time Streaming Protocol (RTSP) underlie delivery of content to the client, since these protocols are well known. It will be appreciated by one skilled in the art that these protocols are discussed herein for exemplary purposes only due to their broad familiarity by artisans and that any protocol providing the signaling characteristics relied upon herein, may be used.

In one aspect, the present invention relates to a system and associated methods for providing at least one media data protection stream, independent of an associated media data stream, and further providing at least one media data hint track to facilitate the transmission of the media data stream over a network and at least one protection data stream to facilitate the transmission of the at least one media data protection stream across the network.

In a related aspect, the present invention is directed to a system and associated methods for allowing an application the freedom to dynamically choose an error protection scheme on demand.

Although the following is addressed in particular to MPEG-4 FGS, it will be clear to a person skilled in the art that the invention can be advantageously applied to any scalable coding scheme.

The principles and operation of method and a system for providing an error-protection scheme over an IP network may be better understood with reference to the drawings and the accompanying description.

FIGS. 1 and 2, discussed below, and the various embodiments used to describe the principles of the present invention in this patent document are by way of illustration

only and should not be construed in any way to limit the scope of the invention. Those skilled in the art will understand that the principles of the present invention may be implemented in any suitably arranged video encoder and decoder.

The present invention provides a novel architecture and specific protocols to provide a capability for providing an adaptive and efficient error protection scheme, for use in a network, such as the one shown in Fig. 1, thereby allowing applications to switch between different error protection strategies dynamically, as will be described.

FIG. 1 illustrates a simplified representation of one embodiment of a system 100 incorporating the invention. As shown, a client 130 and a server 118 are in communication over a network 120. Exemplary system 100 is only one example of a suitable system and is not intended to suggest any limitation as to the scope of use or functionality of the improved methods and apparatuses described herein.

For purposes of illustration, the following description will assume that an audio or video signal has been converted into a digital data stream (a media stream) and is to be transmitted in a network from a source node 110, via a server 118, to a destination node (i.e., client) 130. The description will further assume by way of example that the digital data stream, or payload, has been divided into a sequence of frames or payload packets. According to the embodiment of the present invention, the video encoder (source node) 110 includes a video frame source 112, a video encoder including a base layer encoder 114a and an enhancement layer encoder 114b and an encoder buffer 116. Video frame source 112 may be any device capable of generating a sequence of uncompressed video frames, including a television antenna and receiver unit, a video cassette player, a video camera, a disk storage device capable of storing a "raw" video clip, and the like. The uncompressed video frames, sourced from video frame source 112, enter video encoder 114 at a given picture rate (or "streaming rate") and are compressed according to any known compression algorithm or device, such as an MPEG-4 encoder. Video encoder 114 then transmits the compressed video frames to encoder buffer 116 for buffering in preparation for transmission across data network 120 via server 118. It is noted that video encoder 110 may be executing either external to or within a general purpose server 118.

PHUS020394P

Data network 120 may be any suitable network and may include portions of both public data networks, such as the Internet, and private data networks, such as an enterprise-owned local area network (LAN), metropolitan area network (MAN) or wide area network (WAN).

5 Depending on the application, destination node (client) 130, which receives the streaming media, may be embodied in many different ways, including a computer, a handheld entertainment device, a set-top box, a television, an Application Specific Integrated Circuits (ASIC), and so forth. Destination node (client) 130 includes a decoder buffer 132, a video decoder 134 and a video display 136.

10 FIG. 2 illustrates, by way of example, an architecture and associated protocols for implementing the protection scheme of the invention having ACTs 1-5 shown as A1-A5. ACT 1:

An FGS encoded .mp4 file is shown at act 1 of Fig. 2. The .mp4 file may be encoded such as at the video encoder 112 (See Fig. 1) using FGS techniques wherein a portion of the video data is first used to produce a base layer (BL) 202. An Enhancement layer (EL) 204 is then generated using the motion compensated residual images. Motion compensated residual images are then generated from the video data and base layer (BL) 202 using a fine granular coding technique. As is well known in the art, FGS encoding represents one type of video scalability. Images coded with this type of scalability can be decoded progressively. In other words, the decoder can start decoding and displaying the image without the need for receiving all of the data used for coding that image. As more data is received, the quality of the decoded image is progressively enhanced until the complete information is received, decoded, and displayed.

25 In addition to generating the FGS base layer 202 and enhancement layer 204, in accordance with the principles of the invention, multiple protection data streams are generated, each being dynamically selectable by the client upon demand. There is shown separate and independent protection data streams, each associated with the .mp4 file. A first protection track (EP1) 206 may be constructed, for example, in accordance with the principles of FEC error protection. A second protection track (EP2) 208 may be constructed, for example, in accordance with the principles of retransmission error protection. A third protection track (EP3) 210 may be constructed, for example, in

accordance with a hybrid scheme that incorporates features of FEC error protection and retransmission error protection. Each of the three protection schemes are dynamically selectable by a client upon demand.

ACT 2:

5       The principles of multi-track hinting are taught in co-pending U.S. patent application Ser. No. 60/451,916 filed March 4, 2003, entitled "System and Method for transmitting scalable coded video over an IP network", incorporated by reference herein in its entirety. In accordance with the principles of multi-track hinting taught therein, a pre-processing method, referred to as multi-track hinting, backward compatible with the  
10       current MPEG-4 media file format standard, makes it possible to use a general purpose MPEG-4 streaming server to efficiently stream layered video in accordance with changing channel characteristics, complexity constraints and user preferences. That is, the server, without major modification, is capable of automatically using multiple channels (i.e., RTP connections), thereby providing the streaming system the flexibility  
15       to adapt to network conditions (e.g., available bandwidth) by adjusting the number of scalable layers to be transmitted. As the available network bandwidth decreases, less hint tracks are required by the server because a smaller portion of the video stream is scalably transmitted to comply with the decreased bandwidth.

As shown in Fig. 2, a hinter module 214 generates a hint track (i.e., hint 1) 216a  
20       to facilitate the transmission of the FGS encoded base layer 202 across a data network such as, for example, data network 120. In addition, the hinter module 214 generates a plurality of hint tracks, i.e., (hint tracks 2 - 5) 216b-e, each being associated with enhancement layer (EL) 204.

One feature of the present invention is that each of the protection tracks, i.e., EP1,  
25       EP2 and EP3, may advantageously utilize the principles of multi-track hinting method to thereby provide error protection according to the prevailing network conditions. That is, multiple hint tracks may be used to stream the protection track via multiple RTP connections in much the same manner as is performed for the .mp4 parent data file, as described in co-pending application 60/451,916, referenced above. This flexibility in  
30       streaming the protection track across a network is illustrated by way of example in Fig. 2 where there is shown multiple hint tracks associated with each of the protection tracks,

e.g., EP1-3. Specifically, for the first protection track EP1 206, the hinter 214 generates hint tracks 6 and 7, designated as 216f and 216g. For protection track EP2 208, the hinter 214 generates hint tracks 8, 9 and 10, designated respectively as 216h, 216i and 216j. Associated with protection track EP3 210, the hinter 214 generates a single hint track 11,  
5 216k.

In the present context, the teachings of co-pending application 60/451,916, referenced above, remain true, however, in addition, hint tracks are utilized to transmit protection tracks to protect data streams being transmitted across a network. Specifically, the protection data streams may be scalably transmitted across the network in compliance  
10 with a measured network condition. However, the network condition of note in the present context is not the bandwidth, as is true of the video data stream, but rather the measured packet loss rate. As the packet loss rate is determined to be increasing there is a need or increased error protection. Accordingly, additional hint tracks above the number initially used to facilitate the transmission of the protection data streams will be  
15 utilized to compensate for the measured increase in the packet loss rate.

As a specific example, reference is made to exemplary protection track EP2 208, which has associated with it three hint tracks 8-10, 216h-j, which were generated simultaneous with EP2 208. Assuming that the initially measured packet loss rate is such that only a subset of the three hint tracks are initially required to facilitate the scalable  
20 portion of protection data stream EP2 208 necessary to satisfy a predetermined packet loss threshold, e.g., hint track 8 216h. Assume now that the packet loss rate increases at some point. It may then be required to utilize one or more additional hint tracks associated with protection data stream EP2 208 to compensate for the degraded network condition (i.e., increase in packet loss rate). For example, it may be required at some  
25 point to utilize all three hint tracks 8-10 216h-j to thereby provide the highest scalable portion of protection data stream EP2 208.

The above description is provided to illustrate one feature of the invention. That being, the novel protection data streams may be scalably transmitted across the network in the same manner as the parent video data stream with the distinction being the parent  
30 video stream is scalably modified in accordance with a measured change in network bandwidth while the protection data streams are scalably modified in accordance with the

measured change in packet loss rate. In the former case, when the bandwidth is decreased, less hint tracks are required. Similarly, and in the latter case, when the packet loss rate is decreased, less hint tracks are required.

ACT 3:

5 In accordance with the principles of the invention, the client 130 may, at any point in time, dynamically subscribe or unsubscribe to receive a protection channel. Accordingly, the client 130 needs to monitor its receiving quality and actively trigger the protection channel when it deems necessary. To initiate error protection in accordance with the method of the invention, a client must first be made aware of the type of error  
10 protection available at the server. As such, a mechanism is required to inform clients of the availability and description of the types of error protection that are available from the server. This mechanism is preferably executed by initially performing a Session Description Protocol (SDP) between the client and server.

Generally, SDP is a protocol intended for describing multimedia sessions for the  
15 purposes of session announcement, session invitation, and other forms of multimedia session initiation. It is also maintained by the IETF, and further information regarding SDP is located on the Internet at [www.ietf.org](http://www.ietf.org) in general, and at [www.ietf.org/rfc/rfc2327.txt](http://www.ietf.org/rfc/rfc2327.txt) in particular. The present invention extends the functionality of SDP to include protocols which convey additional information to the  
20 client concerning the availability and characteristics of error protection available from the server.

In operation, the SDP protocol is performed between client and server prior to making a subscription request for a video data file, e.g., an .mp4 file. The SDP protocol session avails the client of various information about the session. Most importantly, the  
25 client is made aware of what options are available regarding error protection. Namely, the types of error protection available, the track numbers and so on. The client stores this information which may then be later used if the client should at some point during the transmission of the video source file, determine that error protection is warranted.

In the event the client makes a determination that error protection is warranted,  
30 the client requests error protection by first making a subscription request to the server using the RTSP protocol. As described above, the RTSP protocol is an application-level

protocol, which offers a session negotiation and content description mechanism. That is, the RTSP protocol describes how to stream content from a server to a client. The request is transmitted across the IP network 120 using a common IP based packet switching technology such as the Transmission Control Protocol (TCP). As is well known in the art, the TCP protocol is a network protocol system that is independent of computer or network operating system and architectural differences. Assuming there is no pre-existing communication channel between the client and the server, a server receives a client subscription request. An exemplary client subscription request may have the following form:

10 Client → Server

```

1.    SET_PARAMETER rtsp://130.140.67.83/sample.mp4 RTSP/1.0
2.    CSeq: 32
3.    Session: 3453643
15  4.    Content-length: 35
5.    Content-type: text/bool/integer
6.    Track 11: 1           //the 11th track is set to be 1 (ACTIVE)
7.    Range: 34521 – 34570   // 50 packets are required, (start seq.
# - end seq. #) //

```

20

Of particular note in the subscription request above, are lines 6 and 7. Specifically, the client has made a subscription request to activate protection track 11 for the range of packets denoted by packet identifiers 34521 – 34570. That is, the client has made a determination that the specific range of packets specified has been corrupted or dropped and wishes to retrieve them via protection channel 11. Protection channel 11 may be synonymous with any number of error protection schemes provided by the server including FEC error protection, retransmission error protection, or a hybrid scheme.

25

With continued reference to FIG. 2, protection channel 11 may be synonymous with protection track EP1 or EP2 or EP3, for example.

30

In response to the client based subscription request, the server may respond to the client with an acknowledgment which may have the following form:

Server → Client

```

1.    RTSP/1.0 200OK
15  2.    CSeq: 32
3.    Date: 28 Jan 2002 15:33:10 GMT

```

35

As emphasized in line 6 of the subscription request above, it should be noted that one feature of the present invention, is the flexibility provided in allowing a client to dynamically select one protection scheme from among a plurality of error protection choices available from the server. This flexibility stands in contrast to prior art approaches which restrict a client to select only a single unchangeable method of error protection, e.g., either retransmission or FEC protection. Advantageously, by maintaining the protection channel(s) as separate distinct data streams apart from the corresponding data stream, multiple error protection options are made available to the client upon demand. Further, by separating protection data from protected data, changing the protection data can change the protection level or strategy, but the protection procedures remain the same.

Next, it will be described in more detail how a client selects a protection scheme from among the protection schemes made available at the server.

In accordance with one embodiment, a protection scheme may be selected by the client via the range parameter (See line 7 above, i.e., Range: 34521 – 34570). That is, whenever the end sequence number in the range, e.g., 34570, is specified to be infinity as part of the request, the server may assume that the client desires an FEC type error protection mode, for example. Alternatively, whenever the end sequence number is equal to the starting sequence number + 1, it may be assumed that the client desires a retransmission type protection mode. If neither of these two options are selected, it is assumed that the client desires a hybrid transmission mode (e.g., a combination of FEC and retransmission), as indicated in the example above (i.e., end sequence number > 1 + starting sequence number and not equal to infinity).

Other modes of selecting a protection scheme, not explicitly recited herein, are also within the contemplation of the invention.

With continued reference to Fig. 2, subsequent to sending the acknowledgment in response to the client subscription request, the server loads the appropriate hint tracks and creates an RTP connection for each hint track. In the example shown, RTP connection 218a is created for hint track 1, 216a, RTP connections 218b-e are created for hint tracks 216b-e, respectively. Assume, for purposes of explanation that protection track EP1 is selected by the client 130, in this case hint tracks 6 and 7, 216f and 216g, respectively are

loaded and RTP connections 218f and 218g are created. It is to be appreciated that additional dedicated RTP connections, e.g., 218f and 218g, are created to facilitate the transfer of protection data.

ACT 4:

5           At act 4, the client 130 creates a corresponding RTP connection to those described above at act 3 to facilitate the transfer of the video data and corresponding protection track data.

ACT 5:

10           At act 5, the transmitted FGS encoded video data streams, i.e., BL 202 and EL 204 are decoded and displayed.

15           The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.

20

**CLAIMS:**

1. A method of transmitting a bit stream across a network from a sending device to a receiving device, the method comprising:
  - 5 a coding act for producing at least one protection bit stream from said bit stream using a channel coding technique; and
  - a generating act for generating at least one hint track from said at least one protection bit stream, wherein said at least one hint track is associated with said at least one protection bit stream in a many-to-one relationship.
- 10 2. The method of Claim 1 further comprising a storing act for storing said at least one protection bit stream and said at least one hint track on a storage medium.
3. The method of Claim 1 further comprising the acts of:
  - 15 receiving from said receiving device an error correction request for error protection; and
  - outputting a first protection bit stream from among said at least one protection bit stream in accordance with associated hint tracks from among said at least one hint track;
  - 20 wherein said first protection bit stream is produced at said coding act and said associated hint tracks are generated at said generating act.
4. The method of Claim 3, further comprising the acts of:
  - 25 subsequently receiving from said receiving device a modified error correction request for error protection in response to a change of network condition; and
  - outputting at least one modified protection bit stream from among said at least one protection bit stream produced at said coding act in accordance with associated hint tracks;
  - wherein said at least one modified protection bit stream is produced at said
  - 30 coding act and said associated hint tracks are generated at said generating act.

5. The method of claim 1, wherein said bit stream is a data stream output in accordance with a source coding method.
6. The method of claim 1, wherein said at least one protection bit stream is a data stream produced in accordance with a data protection coding method.
7. The method of claim 1, wherein said at least one hint track is a data stream generated in accordance with a hinting algorithm.
8. The method of claim 7, wherein said hinting algorithm optimized in accordance with at least a network condition, network protocol and network type.
9. The method of Claim 1, wherein the receiving device is a client device and the sending device is a server device.
10. A computer-readable medium bearing instructions for performing error protection, said instructions being arranged, upon execution by one or more processors, to perform the acts of the method of claim 1.
11. An error protection system, comprising:  
means for producing at least one protection bit stream from said bit stream using a channel coding technique; and  
means for generating at least one hint track from said at least one protection bit stream, wherein said at least one hint track is associated with said at least one protection bit stream in a many-to-one relationship.
12. The error protection system of claim 11, further comprising means for storing said at least one protection bit stream and said at least one hint track on a storage medium.
13. The error protection system of claim 12, further comprising:

means for receiving from said receiving device an error correction request for error protection; and

means for outputting a first protection bit stream from among said at least one protection bit stream in accordance with associated hint tracks from among said at least one hint track;

wherein said first protection bit stream is produced at said coding act and said associated hint tracks are generated at said generating act.

14. The error correction system of claim 13, further comprising:

means for subsequently receiving from said receiving device a modified error correction request for error protection in response to a change of network condition; and

means for outputting at least one modified protection bit stream from among said at least one protection bit stream produced at said coding act in accordance with associated hint tracks;

wherein said modified protection bit stream is produced at said coding act and said associated hint tracks are generated at said generating act.

15. The method of claim 1, wherein said bit stream is a data stream output in accordance with a source coding method.

16. The error correction system of claim 13, wherein said at least one protection bit stream is a data stream produced in accordance with a data protection coding method.

17. The error correction system of claim 13, wherein said at least one hint track is a data stream generated in accordance with a hinting algorithm.

18. The error correction system of claim 13, wherein said hinting algorithm optimized in accordance with at least a network condition, network protocol and network type.

PHUS020394P

19. The error correction system of claim 13, wherein the receiving device is a client device and the sending device is a server device.

PHUS020394P

**ABSTRACT**

A system and method provides a realistic architecture and specifies the protocols that are necessary for carrying out adaptive and efficient protection, thereby allowing applications to dynamically switch between different protection strategies. Protection is  
5 uniquely achieved by providing the protection track (206, 208, 210) as a separate stream from the media data stream (202, 204). In this manner, changing the protection data can change the protection level or strategy, but the protection procedures remain the same. Further, the method uses Real-time Transport protocol (RTSP) instead of Internet Group  
10 Management protocol (IGMP) which can achieve faster protection and provide more flexibility to applications.

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Atty. Docket

QIONG S. LI ET AL.

US 020394

Serial No.

Group Art Unit

Filed: CONCURRENTLY

Examiner

Title: SYSTEM AND METHOD FOR PROVIDING ERROR RECOVERY FOR STREAMING  
FGS ENCODED VIDEO OVER AN IP NETWORK

Commissioner for Patents  
Alexandria, VA 22313-1450

APPOINTMENT OF ASSOCIATES

Sir:

The undersigned Attorney of Record hereby revokes all prior appointments (if any) of Associate Attorney(s) or Agent(s) in the above-captioned case and appoints:

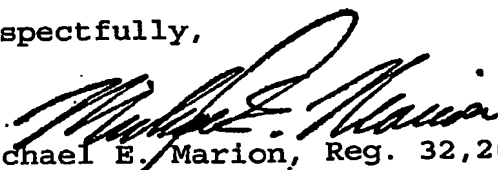
DICRAN HALAJIAN

(Registration No. 39,703)

c/o PHILIPS ELECTRONICS NORTH AMERICA CORPORATION, Intellectual Property Department, 580 White Plains Road, Tarrytown, New York 10591, his Associate Attorney(s)/Agent(s) with all the usual powers to prosecute the above-identified application and any division or continuation thereof, to make alterations and amendment therein, and to transact all business in the Patent and Trademark Office connected therewith.

ALL CORRESPONDENCE CONCERNING THIS APPLICATION AND THE LETTERS PATENT WHEN GRANTED SHOULD BE ADDRESSED TO THE UNDERSIGNED ATTORNEY OF RECORD.

Respectfully,

  
Michael E. Marion, Reg. 32,266  
Attorney of Record

Dated at Tarrytown, New York  
this 1<sup>ST</sup> day of MAY, 2003.  
C:\wp\appasoc.hj.doc

1/2

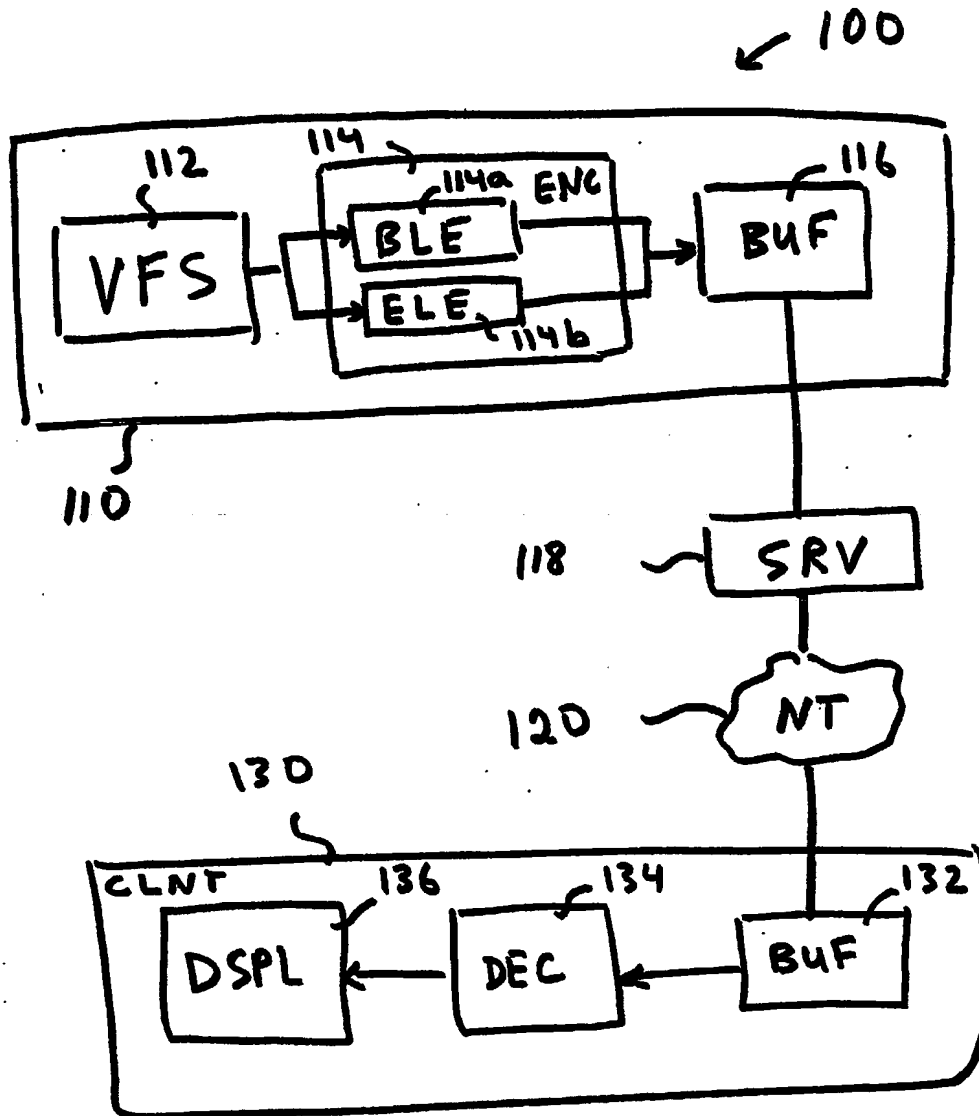


FIG 1

2/2

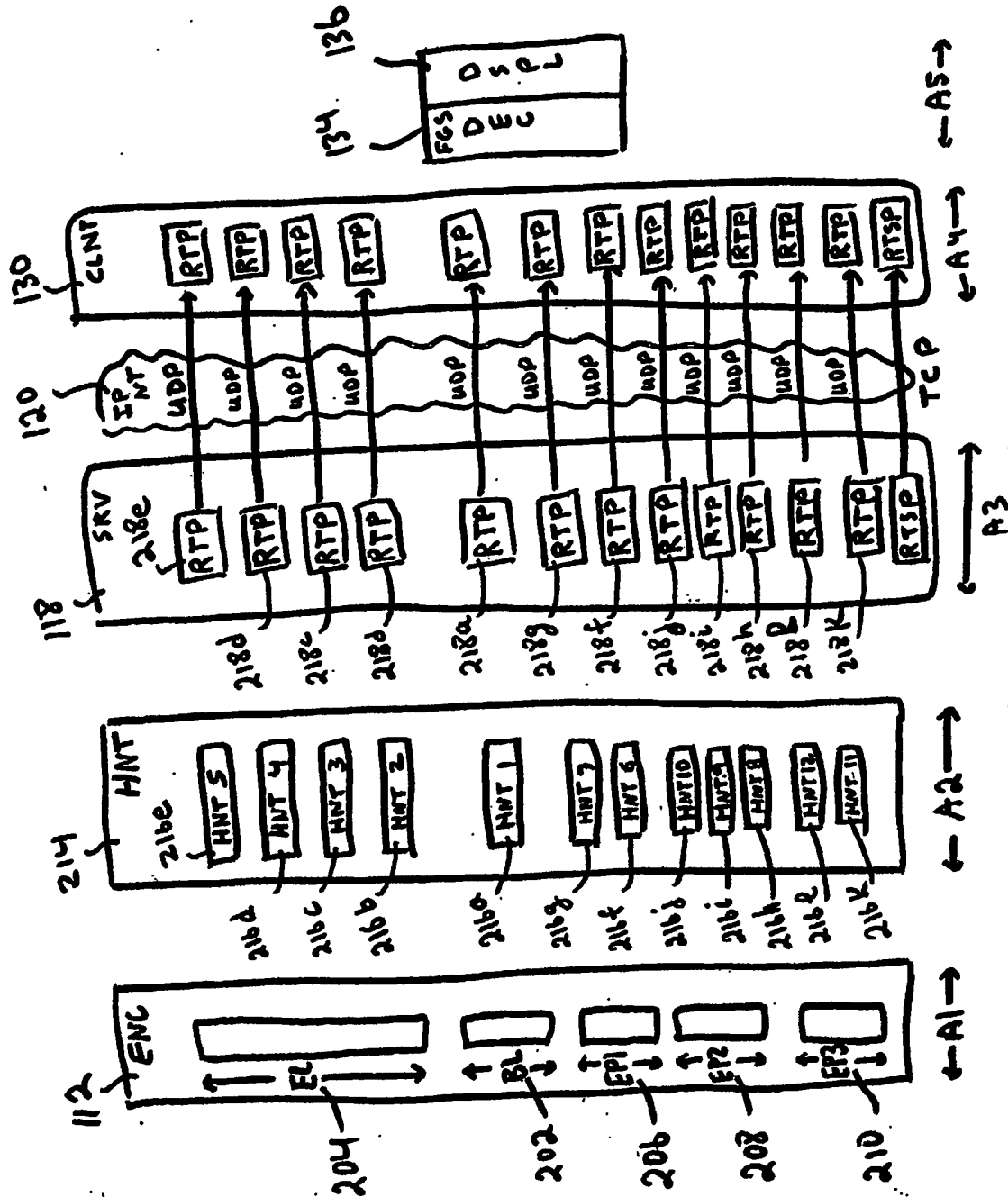


FIG 2

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**